社会化媒体用户信息披露意愿影响模型构建与实证*
——以微信用户为例

郭海玲 马红雨 许泽辉
河北大学管理学院 保定 071002

摘要：［目的/意义］社会化媒体信息隐私泄露事件频繁发生，加剧了用户对信息隐私的担忧，用户在使用社会化媒体过程中是否愿意向平台披露个人信息成为推动社会化媒体平台健康发展的关键。［方法/过程］利用隐私计算理论和沟通隐私管理理论为框架，结合隐私关注，构建社会化媒体用户信息披露意愿影响模型。以微信平台为例，通过问卷调查的方式收集样本数据，使用Smart PLS软件对模型合理性进行验证。［结果/结论］研究发现，感知收益、信任、感知信息控制均正向影响信息披露意愿，隐私关注负向影响信息披露意愿；信任负向影响感知风险；感知信息控制负向影响隐私关注；隐私倾向正向影响隐私关注和感知风险。

关键词：社会化媒体 隐私计算 沟通隐私管理 信息隐私 披露意愿
分类号：G203
DOI：10.13266/j.issn.0252－3116.2019.15.013

1 引言

社会化媒体作为基于用户社会关系的内容生产与交换平台，依赖用户披露的数据和信息得到了快速发展。但近几年，个人信息泄露及信息被非法使用等隐私事件频繁发生，特别是2018年全球最大的在线社交网站Facebook发生用户数据泄露事件之后，产业界和学术界再度掀起关于用户信息隐私的讨论。一方面，社会化媒体平台需要精确地了解用户复杂的隐私需求；另一方面，在鼓励用户披露信息的同时社会化媒体平台也要对用户隐私给予充分的保护和尊重。由此，研究社会化媒体用户信息披露意愿对于帮助商家合理获取和利用用户信息并提供优质服务具有重要意义。

当前国内外学者主要从社会化媒体平台或用户个体行为等视角出发，研究社会化媒体隐私披露问题。研究所采用的理论方法集中在计划行为理论[1]、隐私计算理论[2]、解释水平理论[3]及沟通隐私管理理论[4]等。其中，在信息披露相关理论中隐私计算理论是目前最常用的理论模型。但是随着研究的深入，近年来越来越多的研究表明，社会化媒体用户信息披露意愿并不完全符合隐私计算结果[5]。作为隐私计算理论模型的有益补充，沟通隐私管理理论从另一个角度解释了用户披露信息的过程，该理论通过边界控制来实现隐私披露与隐匿行为的平衡。隐私边界的变化除了受到隐私计算中用户感知风险和收益的影响外，还涉及个体隐私控制权、信任等因素的影响[6]。为了更加全面地探究影响用户信息披露意愿的具体因素，笔者从用户信息披露与隐匿的隐私边界切入，以目前国内最活跃的具有明显强关系特征的社会化媒体——微信平台为例，基于经典的隐私计算理论和沟通隐私管理理论，结合隐私关注，构建社会化媒体用户披露意愿影响因素模型，并通过实证研究对其有效性进行验证。该研究在理论上，为社会化媒体环境下用户信息披露意愿提供了新的研究视角，实践上为社会化媒体平台和公共管理者采取有效的用户信息隐私保护措施提供了参考依据，同时为社会化媒体平台运营商更好地完善其应用，进而提升竞争力和影响力，保障社会化媒体健康快速发展提供了理论指导。

2 理论基础

2.1 隐私计算理论

隐私计算理论由R. S. Laufer和M. Wolfe在1977

＊ 本文系国家社会科学基金青年项目“跨境电子商务信息服务协同创新模式研究”（项目编号：17CTQ046）研究成果之一。
作者简介：郭海玲（ORCID：0000－0003－1487－9725），副教授，博士，E-mail：guohailing1@163.com；马红雨（ORCID：0000－0001－5834－9852），硕士研究生；许泽辉（ORCID：0000－0002－2851－5386），硕士研究生。
收稿日期：2018－12－05 修回日期：2019－03－01 本文起止页码：111－120 本文责任编辑：徐健

年首次提出并逐渐发展起来[7]。该理论认为用户在进行信息披露时会进行风险与收益比较，只有当感知收益大于风险时用户才会进行信息披露。经过十多年的发展，学术界对隐私计算理论的研究已经比较成熟，且被广泛用于不同情境下的隐私披露问题研究[1]。其中，电子商务[8]、社交媒体[9]、医疗健康[10]领域都是当前热点的研究情境。有研究表明虽然都是基于隐私计算理论框架，但是不同情境下的用户还是会表现出不同的隐私披露意愿[11]。微信是以强关系社交网络为主，在该情境下强关系群体既是信息获取的重要来源，也是隐私泄露的主要源头。笔者选取微信平台为研究对象，分析个体在使用社会化媒体平台时对感知收益和感知风险权衡的隐私决策过程。

2.2 沟通隐私管理理论

沟通隐私管理理论（Communication Privacy Management Theory，CPM）由 S. Petronio 在 1991 年提出，是研究用户披露或隐匿个人信息决策的系统性理论。该理论指出私人与公共之间存在着隐私边界，而这个隐私边界是保护其个人信息的关键[6]。隐私倾向作为影响边界规则形成的主要因素，反映了个人管理其隐私边界开放和封闭的内在需要，其被定义为个人保留信息隐私空间或限制披露个人信息的总体倾向[12]。隐私倾向较高的个体往往更关心个人边界，需要更多地控制个人信息。另外，控制和信任作为沟通隐私管理理论的两大核心[6]，也会在一定程度上影响用户隐私边界的形成。其中，控制可以理解为用户对隐私界限的把握，在社会化媒体中表现为用户认为能够按照自身意愿对已发布信息进行控制的能力[13]。在实践中，越来越多的社会化媒体平台为用户开放了更多更细致的隐私控制权限，其真实意图遭到外界质疑，隐私控制权限的赋予是否真的有利于用户保护个人信息隐私，抑或是社会化媒体平台另有所图，为验证其对用户信息披露意愿的具体影响，引入信息控制变量。考虑到笔者研究的是用户信息披露意愿，有学者指出对于态度意愿来说，感知控制比实际控制更加重要[14]，所以模型中选择感知信息控制变量，它是对个人实际信息控制的主观感受，是基于实际控制的心理状态。此外，信任作为一种心理信念，有助于打破隐私边界的形成，用户的信任度越高，对其隐私边界的开放程度越高，在一定程度上会影响到用户的信息披露意愿[6]。在社会化媒体平台中用户之间的交互性较强，其内容表达更多基于信任感、隐私性，这些都是影响隐私边界变动不容忽视的关键因素，所以沟通隐私管理理论同样适用微信平台。

2.3 隐私关注

隐私关注由信息系统专家 H. J. Smith 等于 1996 年提出并将其定义为“由于可能损失信息而引起的担忧”[15]。它可作为用户对涉及个人私密事项等隐私情境的一种主观认识和感受，揭示了在不同影响因素的作用下，用户通过衡量、评估隐私价值而做出决策的行为[16]。作为一个多维概念，H. J. Smith 将隐私关注划分为收集、错误、未经授权的二次使用和不适当访问 4 个维度[15]。N. K. Malhotra 等认为互联网隐私关注包括收集、控制和知情 3 个维度[17]。

因社会化媒体具有用户高度的参与性、社交性和公开性，为更有效地表征和检验用户在该情境下的隐私关注行为，笔者将探究隐私关注在社会化媒体用户个人信息披露过程中的作用机制。

3 研究假设与模型构建

3.1 感知风险

感知风险被定义为个体将信息披露给相关主体时所感知到的潜在损失[17]。由于信息本身及信息接收主体的不确定性，导致用户在社会化媒体平台披露的个人信息可能会被不法分子滥用，致使披露风险增加。在社会化媒体平台中用户的感知风险主要表现为信息的内部泄露和贩卖，非授权的访问、窃取和使用等。R. Chen 等研究社交网络用户信息披露意愿时发现，用户感知风险越大，其个人信息披露意愿越消极[18]。P. A. Norberg 在研究消费者隐私悖论行为成因时指出，用户感知到的风险对其隐私披露意愿有显著的负向影响[19]。N. Hajli 等在研究 Facebook、Twitter 和 LinkedIn 等社交平台安全性对美国用户隐私态度的影响时发现，感知风险负向影响用户的信息披露态度[20]。因此，笔者假设：

H1：感知风险负向影响信息披露意愿

3.2 感知收益

感知收益被定义为信息披露后所带来的经济收益、个性化服务、社会融入与适应等对个体有利的价值感知[21]。在社会化媒体平台上，用户的感知收益主要来源于与其他用户共享信息所带来的愉快感和融入感。H. Krasnova 等研究了跨文化环境下社交网站用户信息披露行为，结果发现虽然存在文化差异，但是用户披露信息时感知到的收益对披露意愿的影响都是正向显著的[22]。李纲研究新浪微博用户个人信息披露态度时表明，感知收益对用户披露态度有正向影响[23]。T. Wang 等在研究消费者通过移动应用程序披

露个人信息问题时，表明感知收益与用户信息披露意愿正向相关[24]。因此，笔者假设：

H2：感知收益正向影响信息披露意愿

3.3 信任

信任是社会关系中的重要因素，其在不确定性较高的互联网环境中发挥着重要作用。如果用户相信服务商，就会认为社会化媒体平台会关心用户利益，进而对社会化媒体平台产生依赖并愿意披露个人信息[25]。兰晓霞等指出在移动社交环境下大学生的信任主要来自社交网站及网站用户[26]。李琪等研究发现在微信环境下，用户对平台的信任正向影响其自我披露意愿，但在微博环境下，信任对自我披露意愿的影响并不显著[27]。R. Chen 基于社会资本理论视角，构建了社交网络用户自我披露意愿模型，文章主要选取 Facebook 用户为调研对象，分析结果表明美国社交网络用户对其他成员的信任会对信息披露行为产生积极影响[18]。本研究认为当用户对社会化媒体平台运营者及其他用户处于信任状态时，会不自觉地降低自我保护意识，拓展隐私开放边界，增加披露意愿。因此，笔者假设：

H3：信任正向影响信息披露意愿

信任是指用户相信另一方不会产生机会主义行为的信念[28]。用户在使用社会化媒体共享信息过程中，感知到的风险是阻碍用户进行信息披露的主要原因，而信任的存在可以降低用户对这些风险的感知。C. Moorman 等认为，信任会减少感知的不确定性，进而降低感知风险[29]。S. L. Jarvenpaa 和 N. Tractinsky 在研究跨文化网络零售问题时，发现感知信任对感知风险有负面影响[30]。因此，笔者假设：

H4：信任负向影响感知风险

3.4 隐私关注

隐私关注是一种与隐私泄露相关联的信息意识和感知，是个人在特定隐私情境下的主观感受[31]。有研究表明，个人信息的披露意愿会随着隐私关注的逐渐提高而不断降低[32-33]。如朱候等研究社交网络用户隐私关注与隐私披露的关系时，发现隐私关注在一定程度上负向影响用户披露意愿[34]。K. Yang 研究在线医疗服务系统使用意愿时发现，对个人医疗隐私信息的关注会导致用户不愿意提供个人医疗信息或提供虚假的医疗信息[35]。因此，笔者假设：

H5：隐私关注负向影响信息披露意愿

隐私关注反映了个体对可能失去信息隐私的内在担忧，会对用户的信任产生一定影响。例如，N. K. Malhotra 在研究互联网用户隐私关注时指出，基于互联网的隐私关注负向影响与信任相关的信念[17]。张晓娟等研究也发现，智能手机用户隐私关注越强，对智能手机的信任度越低[36]。因此，笔者假设：

H6：隐私关注负向影响信任

3.5 感知信息控制

感知信息控制代表在社会化媒体平台上用户感知到的对个人信息掌控能力的容易程度。当个体拥有执行信息披露控制行为相关的资源或机会越多时，其感知信息控制水平越高。增强用户对个人信息的控制能力，可以在一定程度上弱化用户的隐私关注[37]。张会平等对微信用户隐私关注的影响因素进行实证分析后，发现用户的感知信息控制负向影响其隐私关注[38]。因此，笔者假设：

H7：感知信息控制负向影响隐私关注

当个人信息上传到社会化媒体平台后，信息主体就失去了对隐私信息的部分控制权，只能被动接受平台运营商对个人信息的掌控，并承担隐私随时遭受侵犯的风险。用户的感知信息控制水平越高，其越能决定信息披露的类型及范围，这在一定程度上可限制甚至消除源自隐私泄露的风险。N. Hajli 等学者研究 Facebook、Twitter 和 LinkedIn 等社交平台用户信息披露影响因素时发现用户感知信息控制越强，用户感知风险越低[20]。由此，笔者假设：

H8：感知信息控制负向影响感知风险

毫无疑问，对个人信息的控制在信息隐私研究领域扮演着重要的角色。一旦个体意识到他们拥有更多的控制权来管理信息隐私时，用户很可能会扩大信息隐私的边界，提高信息披露意愿。李纲等研究新浪微博用户个人信息隐私披露意愿时发现，只有当用户的感知信息控制能力越强时，其披露意愿才会越强烈[23]。H. Cavusoglu 等研究隐私政策变更对 Facebook 用户信息披露意愿的影响时发现，给予用户更多的隐私控制权限，就会增加其公开信息的行为[37]。因此，笔者假设：

H9：感知信息控制正向影响信息披露意愿

3.6 隐私倾向

隐私倾向是指个人保留其信息隐私空间或限制披露个人信息的总体倾向[12]。隐私倾向越高的个体对潜在的隐私威胁越敏感，越关注自己的隐私边界。H. Xu 等研究个人感知与机构隐私保障问题时发现隐私倾向正向影响用户的隐私关注[12]。张会平等在研究微信用户信息隐私关注的形成机制时，也验证了隐私倾向对隐私关注的正向作用[38]。因此，笔者假设：

H10:隐私倾向正向影响隐私关注

在其他因素保持不变时,较低的隐私倾向产生的直接结果是用户对信息泄露的风险重视不足,其对风险的感知时长仅停留在近期,而无法预判隐私泄露带来的长远性风险,甚至认为只要个人财产没有受到侵害就不算是风险。针对两者的关系,Z. Liu等研究发现,对于隐私倾向较高的个体而言,其在信息披露时感知的风险会更大[39]。李凯在研究LBS用户信息公开意愿影响因素时发现对隐私的敏感倾向与LBS用户的感知风险呈正相关关系[40]。

H11:隐私倾向正向影响感知风险

基于上述分析,本文所构建概念模型框架见图1。

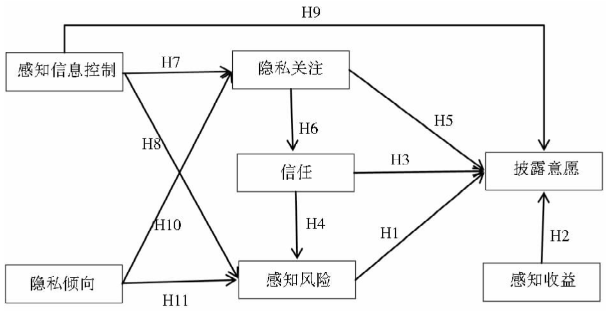


图1 研究模型

4 研究设计

4.1 问卷设计

本研究的问卷主要包括两部分。第一部分是关于微信用户信息披露意愿影响因素的调查,包括感知信息控制、隐私倾向、隐私关注、信任、感知风险、感知收益、披露意愿7个潜变量;第二部分是被调查对象的人口统计变量,包括性别、年龄、学历、使用微信的次数等。对于量表的设计,本研究测量指标均沿用或改编自前人研究,并结合国内微信用户的实际情况进行了适当修改。问卷的具体测量变量及参照来源见表1,所有问项均采用李克特五级量表。本研究以国内知名社交平台微信用户为数据采集样本,通过问卷调查方法进行数据收集,并运用Smart PLS软件对研究模型进行实证检验。

表1 量表测度项及来源

潜变量	测量变量	来源
感知信息控制(PIC)	PIC1. 我认为我能控制谁可以访问我在微信平台上发布的个人信息	H. Xu,T. Dinev 等[41]
	PIC2. 我认为我能控制我的个人信息在微信平台上用于何种目的	
	PIC3. 我认为我能控制微信平台收集我的何种信息	
	PIC4. 总体而言,我认为我能控制已提供给微信平台的个人信息	
隐私倾向(DTVP)	DTVP1. 与其他用户相比,我对微信平台处理我个人信息的方式更加敏感	H. J. Smith[15]
	DTVP2. 对我而言,使用微信平台时保护个人信息隐私是最重要的	
	DTVP3. 与其他用户相比,我更担心微信平台所存在的个人信息隐私威胁	
隐私关注(PC)	PC1. 我比较关注微信平台是否采取措施来防止非授权用户对我个人信息的访问	N. K. Malhotra[17]和
	PC2. 对我来说,知道我的个人信息如何被使用是非常重要的	H. J. Smith[15]
	PC3. 当微信平台要我提供个人信息时,我通常会感到烦恼	
	PC4. 我担心微信平台在没有获得我授权的情况下与其他服务商共享我的个人信息	
信任(T)	T1. 我认为微信平台会合理地使用我的个人信息	J. Fogel[42]、N. K. Malhotra[17]、
	T2. 我认为微信平台能够履行承诺,遵守隐私保护政策	H. Krasnova[43]
	T3. 我认为微信平台上的其他用户是值得信赖的	
	T4. 总体而言,我认为微信平台是值得信赖的	
感知风险(PR)	PR1. 我认为向微信平台提供我的个人信息可能会带来潜在损失	P. A. Pavlou[44]
	PR2. 我认为向微信平台提供我的个人信息可能会被其不恰当的使用	
	PR3. 我认为向微信平台提供我的个人信息可能会出现意想不到的问题	
	PR4. 总体而言,我认为向微信平台提供我的个人信息是有风险的	
感知收益(PB)	PB1. 在微信平台上提供一些个人信息有利于我享受到想要的服务	F. Kehr[45]
	PB2. 在微信平台上提供我的个人信息能使我更容易的融入社交网络群体中	
	PB3. 在微信平台上提供的个人信息能使我更好的与人交流,认识志趣相投的朋友	
	PB4. 总体而言,我认为在微信平台上提供我的个人信息对我是有益的	
披露意愿(DW)	DW1. 在合适的时机,我打算向微信提供个人信息	P. G. Schierz[46]
	DW2. 将来,我很有可能向微信平台提供个人信息	
	DW3. 将来,我愿意向微信平台提供个人信息	

4.2 数据采集

本次问卷通过网络平台问卷星进行发放，发放日期为2018年10月9日至10月25日，共收回问卷477份，剔除无效问卷后，得有效问卷415份，问卷有效率达87%。本研究样本的人口统计特征见表2，表中的频数为调查对象的人次，频率为某类对象占总样本的百分比。表2所呈现的被调查对象特征与《2017年中国移动社交用户洞察报告》中移动社交用户样本特征基本一致[47]。

表2　样本用户统计

样本统计特征	类别	频数	频率	样本统计特征	类别	频数	频率
性别	男	190	45.78%	月收入	1500以下	218	52.53%
	女	225	54.22%		1500－2500	30	7.23%
年龄	18岁以下	16	3.86%		2500－3500	40	9.64%
	18－29岁	372	89.64%		3500－4500	39	9.4%
	30－39岁	20	4.82%		4500以上	88	21.2%
	40－49岁	7	1.69%	使用微信的时间	1年以下	37	8.92%
	50岁以上	0	0%		1－2年	49	11.81%
学历	高中及以下	11	2.65%		2－3年	71	17.11%
	专科	30	7.23%		3－4年	81	19.52%
	本科	286	68.92%		4年以上	177	42.65%
	硕士	77	18.55%	每次使用微信的时长为	低于5分钟	59	14.22%
	博士	11	2.65%		6－15分钟	106	25.54%
使用微信的频次	每天多次	337	81.2%		16－30分钟	63	15.18%
	每天一次	60	14.46%		30分钟以上	187	45.06%
	两三天一次	12	2.89%				
	一周或更久一次	6	1.45%				

4.3 数据分析

4.3.1　信度效度分析　信度反映了问卷的可靠性、稳定性和一致性。笔者选用克伦巴赫系数(Cronbach's Alpha)以及组合信度(Composite Reliability，CR)指标来检验问卷的信度。一般认为，Cronbach's Alpha、CR值超过0.7为内部一致性水平较好。本研究测量模型中每个潜变量的Cronbach's Alpha系数以及CR值均超过了0.7，说明问卷具有较高的信度。效度反映了测量结果的有效性程度。笔者采用聚合效度和区分效度共同检验数据的有效性。一般认为测量变量的因子载荷大于0.7且平均萃取方差(AVE)大于0.5为聚合效度达标。统计结果显示本研究量表具有较好的聚合效度(见表3)。区分效度的检验标准通常是每个潜变量的平均萃取方差的平方根(表4斜对角线元素)大于其与其他潜变量之间的相关系数(表4非对角线系数)。测量结果表明，本研究各潜变量间存在显著差异，区分效度良好。

4.3.2　路径分析与假设检验　本研究采用Smart PLS对研究模型进行路径参数估计，利用Bootstrapping重复抽样的方法检验路径系数的显著性，抽样次数为500次，表5和图2分别给出了路径系数和研究假设的

表3　信度及聚合效度检验

潜变量	测量变量	因子载荷	Cronbach's Alpha	CR	AVE
感知信息控制(PIC)	PIC1	0.779	0.853	0.900	0.693
	PIC2	0.881			
	PIC3	0.833			
	PIC4	0.833			
隐私倾向(DTVP)	DTVP1	0.769	0.804	0.884	0.719
	DTVP2	0.864			
	DTVP3	0.906			
隐私关注(PC)	PC1	0.835	0.872	0.913	0.724
	PC2	0.889			
	PC3	0.822			
	PC4	0.855			
信任(T)	T1	0.860	0.851	0.899	0.691
	T2	0.895			
	T3	0.721			
	T4	0.840			
感知风险(PR)	PR1	0.866	0.907	0.935	0.782
	PR2	0.888			
	PR3	0.898			
	PR4	0.886			
感知收益(PB)	PB1	0.815	0.867	0.909	0.714
	PB2	0.878			
	PB3	0.840			
	PB4	0.845			
披露意愿(DW)	DW1	0.894	0.900	0.938	0.834
	DW2	0.934			
	DW3	0.911			

表 4 区分效度检验结果

变量	感知信息控制	隐私倾向	隐私关注	信任	感知风险	感知收益	披露意愿
感知信息控制	0.832						
隐私倾向	0.279	0.848					
隐私关注	0.127	0.729	0.851				
信任	0.465	0.151	0.052	0.831			
感知风险	0.050	0.468	0.608	-0.093	0.885		
感知收益	0.345	0.177	0.153	0.475	0.066	0.845	
披露意愿	0.313	0.006	-0.036	0.446	-0.094	0.510	0.913

数据分析结果，通过计算路径系数来分析论文中所得假设的合理性。

表 5 假设检验结果说明

假设	关系	路径系数 β	T 值	P 值	检验结果
H1	感知风险→披露意愿	-0.051	0.776	0.219	拒绝
H2	感知收益→披露意愿	0.393	7.300	0.000	接受
H3	信任→披露意愿	0.217	3.619	0.000	接受
H4	信任→感知风险	-0.162	2.373	0.009	接受
H5	隐私关注→披露意愿	-0.087	1.701	0.045	接受
H6	隐私关注→信任	0.052	0.755	0.225	拒绝
H7	感知信息控制→隐私关注	-0.083	2.258	0.012	接受
H8	感知信息控制→感知风险	-0.013	0.228	0.410	拒绝
H9	感知信息控制→披露意愿	0.090	1.750	0.040	接受
H10	隐私倾向→隐私关注	0.752	24.912	0.000	接受
H11	隐私倾向→感知风险	0.497	10.366	0.000	接受

模型的路径检验结果如图 2 所示。感知风险对披露意愿的影响在本研究中未得到数据支持，因此假设 H1 不成立；感知收益对披露意愿有显著正向影响（β = 0.393，P < 0.001），因此假设 H2 得到支持；信任对披露意愿有显著正向影响（β = 0.217，P < 0.001），对感知风险有显著负向影响（β = -0.162，P < 0.01），假设 H3 和 H4 得到支持；隐私关注对披露意愿有负向影响（β = -0.087，P < 0.05），而对信任的影响未通过检验，因此假设 H5 成立，H6 不成立；隐私倾向对隐私关注（β = 0.752，P < 0.001）、感知风险（β = 0.497，P < 0.001）均有显著正向影响，因此假设 H10 和 H11 得到支持。

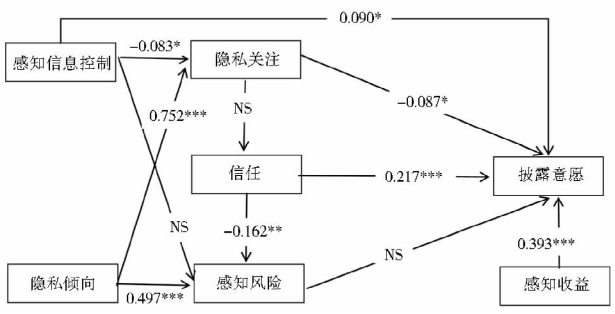


图 2 研究模型路径系数

注：* 表示 P < 0.05，** 表示 P < 0.01，*** 表示 P < 0.001，NS 表示 non-significant

5 研究结论

根据上述对社会化媒体用户信息披露意愿影响因素模型的假设验证，对潜变量间关系及其路径系数进行分析，得出以下结论：

5.1 感知收益对披露意愿有显著正向影响

这表明用户使用社会化媒体获得的服务、社会融入感及愉悦感等促进了用户的信息披露意愿，这与 H. Krasnvovah 等的研究结果一致[22]。然而感知风险对用户披露意愿的负向影响在本研究中未得到数据支持。究其原因主要有：①作为中国主流的社交媒体工具，微信主要是基于用户之间内在情感而建立的社交网络，它有别于基于契约关系形成的社交平台。在以情感为纽带的社交环境中，用户即使知道披露信息会存在一定的风险但也愿意实施披露行为。②用户在使用微信披露个人信息时，一般披露的是一些非敏感性信息，如人口统计特征信息，较少涉及切身利益的敏感信息，如财务信息、医疗记录信息等，同时，用户在该平台披露的多数信息可能在注册或使用其他平台时已有过披露行为，所以不会因为在微信平台中再次披露而给信息主体带来额外风险。③用户对风险感知一般存在滞后性，因大多数用户在微信平台中未有严重的隐私侵犯经历，所以其对风险的感知时长只停留在眼前，而无法预判隐私泄露带来的长期危害，最终使得用户为享受更多的增值服务而选择披露信息。

5.2 信任负向影响感知风险

信任作为一种心理认知会削弱披露所引发的风险，缩小信息封闭边界，扩大信息共享边界，即当用户对社会化媒体存在更多的信任时，其会认为平台诚实可信且有能力保护用户隐私信息安全，这在一定程度上会弱化用户对披露信息所带来的风险信念，这一结论与 C. Moorman 等研究一致[29]。同时，信任是社会关系的重要因素，其作为积极情感倾向会在一定程度上提高用户披露个人信息的意愿。

5.3 隐私关注负向影响披露意愿

该结论与 N. K. Malhotra 等研究一致[17]。用户对社会化媒体的隐私关注，主要源自社会化媒体平台对个人信息的不当收集、非法使用、未经授权而将信息出售给"第三方"等潜在威胁。对于相同的隐私状况，隐

私关注较高的用户主动披露信息的行为会明显减少。此外，隐私关注对信任的影响未通过显著性检验，这是因为不管用户的隐私关注度如何，作为国内主流社交工具，微信平台具有良好的用户隐私保护责任感，会采用数据脱敏等隐私保护技术来保障用户信息安全，因此用户在使用过程中一般对其具备较高的信任感。

5.4 感知信息控制正向影响披露意愿

该结论表明给予用户更多的信息掌控能力，会增加用户的信息披露意愿。感知信息控制水平越高，意味着用户拥有越多控制隐私边界的自主性，从而会不自觉地降低自我保护意识，开放隐私边界，共享更多私密信息，这一结论与李纲研究一致[23]。实证分析结果还表明感知信息控制负向影响隐私关注。该结论表明感知信息控制的增强，意味着其他主体不能随意获取和使用用户个人信息，弱化了因不当收集、未经授权使用个人信息等引起的隐私担忧，这一结论与张会平等研究一致[38]。感知信息控制对感知风险的影响未通过实证检验。究其原因，主要是社会化媒体平台越来越注重用户的细致化隐私控制，增加了朋友圈权限设置、展示动态设置、授权登录管理等功能，使得用户能够更好地管理自己所披露的信息，故而在一定程度上忽略了对风险的感知。

5.5 隐私倾向正向影响隐私关注和感知风险

这与 H. Xu 等的研究结论一致[12]。研究结果表明，隐私倾向越高的用户对隐私的认识越深入，他们会更多地表达对隐私权利的支持，且对于提供隐私带来的不良后果表现得更加谨慎并给予较高的隐私关注。此外，隐私倾向较高的用户往往更易产生焦虑、怀疑等负面情绪，他们对于信息披露带来的潜在隐私威胁更加敏感，因此感知到的风险更高。

6 管理启示

上述研究结论对公共管理者及社会化媒体平台在日后制定用户信息隐私保护政策及采取相关措施时，可提供以下启示与参考：

6.1 增强用户的感知信息控制能力

①改变目前社会化媒体平台流于形式的隐私政策，因为用户极少会投入时间仔细阅读隐私条款，因此平台运营商有必要采取新的措施提升用户对信息的控制能力，如细化隐私设置功能、强化隐私信息提醒服务功能；②平台应加大用户对个人信息处置的力度，赋予用户查询、删除、封锁及更正个人信息，自行设置信息存储时长等权利，增加个人信息的可控性；③加强用户个人在技术层面的信息素养，如让用户明晰平台的隐私政策声明、熟知平台的隐私设置功能，减少因信息不对称而带来的感知信息控制与实际控制之间的差异。

6.2 降低用户信息隐私关注

①平台应不断改进隐私信息保护等核心技术，并鼓励用户采取防御性保护措施，如采用数据脱敏技术、匿名保护身份，精细化信息显示时间等，降低用户在进行个人信息披露时产生的焦虑感；②社会化媒体平台应该完善加密体系，有效预防因不法分子对用户数据的入侵而引发的用户对于隐私泄露问题的担忧；充分尊重用户的知情权，与用户之间的信息交互要透明，及时告知用户信息的使用方式、使用目的和范围以及拒绝提供信息的后果等事项；同时，恪守职业道德，承诺不会在未经用户同意的情况下将个人信息泄露给第三方；③目前我国针对个人信息保护的法律法规呈现出分散立法的趋势，加快推进出台全国统一的《个人信息保护法》可以降低个人信息泄露带来的隐含风险，消除用户顾虑，减轻用户隐私关注度。

6.3 增强用户信任

①社会化媒体平台在日常的运营中应该树立良好的形象，保障所收集用户个人信息的安全，通过有效的事前防范和事后补救来大幅提升用户对平台的信任度；②平台应该制定清晰合理的隐私政策，在用户协议或者服务协议中单独列出“个人信息保护”等相关条款，也可以单独制定个人信息隐私保护规则，并详细说明在获取、管理及保护用户个人信息方面的政策及措施；③合理恰当地使用用户交互界面设计，加强用户之间的沟通交流，改变以往被动的隐私保护观念，注重用户在使用平台时反馈的隐私保护需求，进一步完善相关隐私设置。

6.4 增强用户感知收益

①社会化媒体运营商应该注重特色交友功能的开发，如搭建一些功能友好的社区板块、举办线上线下活动帮助用户扩大其好友圈子等；②为用户提供更具优质便捷的产品和服务，在妥善解决用户信息安全和隐私保护的前提下，充分利用大数据技术进行用户画像，实现个性化推荐，提升用户感知收益。在数据分析过程中，要特别注意做好数据脱敏工作，目前主流技术包括水印、失真、归并、泛化和加密等；③丰富用户之间的交互形式，通过策划更多的可以加强用户情感沟通的互动活动来让用户获取良好的体验价值，如邀请专家、明星、意见领袖等 VIP 用户参与平台举办的交流会，通过互动、交流、创建和应用知识来提高用户感知收益。

7 结语

本研究从用户个体认知角度出发，整合隐私计算理论、沟通隐私管理理论和隐私关注，构建了社会化媒体用户披露意愿影响因素模型，并以中国主流社交媒体平台微信为例，通过实证研究对模型假设的有效性进行了验证。研究结论对社会化媒体平台和公共管理机构建立针对个人信息的隐私保护机制，以及平台运营者完善应用优化服务提供一定的借鉴和参考。

但本研究还存在一些局限性和尚待深究的问题：①根据信息的不同性质，可以对用户个人信息进行分类，不同类型的信息用户会有不同的隐私倾向，会表现出不同的隐私关注度。本研究对个人信息未作细分，未来可基于不同的信息类型对用户的信息披露意愿做更加细化的研究。②本研究未考虑人口统计学特征因素（如年龄、收入、教育背景等）对信息披露意愿的影响，事实上它们之间存在着密不可分的联系，未来将针对该问题做更加深入的挖掘。③隐私披露意愿具有较强的情境性，笔者仅考虑了微信这一强关系社交网络平台情境，不同的社会化媒体平台对用户隐私决策的影响不同，未来将针对不同的社会化媒体平台分别进行探究。

参考文献：

[1] 孙霄凌，程阳，朱庆华. 社会化搜索中用户隐私披露行为意向的影响因素研究[J]. 情报杂志，2017，36(10)：172－179，201.

[2] LI H，SARATHY R，XU H. Understanding situational online information disclosure as a privacy calculus[J]. Journal of computer information systems，2010，51 (1)：62－71.

[3] HALLAM C，ZANELLA G. Online self-disclosure：the privacy paradox explained as a temporally discounted balance between concerns and rewards[J]. Computers in human behavior，2017，68 (C)：217－227.

[4] 王波伟，李秋华. 大数据时代微信朋友圈的隐私边界及管理规制——基于传播隐私管理的理论视角[J]. 情报理论与实践，2016，11(39)：37－42.

[5] CHOI B C F，LAND L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage[J]. Information & management，2016，53(7)：868－877.

[6] EASTIN M S，BRINSON N H，DOOREY A，et al. Living in a big data world：predicting mobile commerce activity through privacy concerns[J]. Computers in human behavior，2016，58(C)：214－220.

[7] LAUFER R S，WOLFE M. Privacy as a concept and a social issue：a multidimensional developmental theory [J]. Journal of social issues，1977，33(3)：23－42.

[8] ZHU H，OU C X J，VAN DEN HEUVEL W J A M，et al. Privacy calculus and its utility for personalization services in e-commerce：an analysis of consumer decision-making[J]. Information & management，2017，54(4)：427－437.

[9] DIENLIN T，METZGER M J. An extended privacy calculus model for SNSs：analyzing self-disclosure and self-withdrawal in a representative US sample[J]. Journal of computer-mediated communication，2016，21(5)：368－383.

[10] 王瑜超. 在线医疗社区用户健康隐私信息披露意愿的影响因素研究[J]. 信息资源管理学报，2018，8(1)：93－103，113.

[11] 王晰巍，相甍甍，张长亮，等. 新媒体环境下信息隐私国内外研究动态及发展趋势[J]. 图书情报工作，2017，61(15)：6－14.

[12] XU H，DIENEY T，SMITH J，et al. Information privacy concerns：linking individual perceptions with institutional privacy assurances [J]. Journal of the association for information systems，2011，12 (12)：798－824.

[13] DINEV T，XU H，SMITH J H，et al. Information privacy and correlates：an empirical attempt to bridge and distinguish privacy-related concepts[J]. European journal of information systems，2013，22 (3)：295－316.

[14] AJZEN I. Attitudes，personality，and behavior[M]. Chicago：Dorsey Press，1988.

[15] SMITH H J，MILBERG S J，BURKE S J. Information privacy：measuring individuals' concerns about organizational practices[J]. MIS quarterly，1996，20 (2)：167－196.

[16] 胡昌平，仇蓉蓉. 虚拟社区用户隐私关注研究综述[J]. 情报理论与实践，2018，41(12)：149－154.

[17] MALHOTRA N K，KIM S S，AGARWAL J. Internet users' information privacy concerns (IUIPC)：the construct，the scale，and a causal model[J]. Information systems research，2004，15(4)：336－355.

[18] CHEN R. Living a private life in public social networks：an exploration of member self-disclosure [J]. Decision support systems，2013，55(3)：661－668.

[19] NORBERG P A，HORNE D R，HORNE D A. The privacy paradox：personal information disclosure intentions versus behaviors [J]. Journal of consumer affairs，2007，41(1)：100－126.

[20] HAJLI N，LIN X. Exploring the security of information sharing on social networking sites：the role of perceived control of information [J]. Journal of business ethics 2016，133(1)：111－123.

[21] STONE E F，STONE D L. Privacy in organizations：theoretical issues，research findings，and protection mechanisms[J]. Research in personnel and human resources management，1990，8(3)：349－411.

[22] KRASNOVA H，VELTRI N F，GUNTHER O. Self-disclosure and privacy calculus on social networking sites：the role of culture[J]. Business & information systems engineering，2012，4(3)：127－135.

[23] 李纲，王丹丹. 社交网站用户个人信息披露意愿影响因素研究：以新浪微博为例[J]. 情报资料工作，2015，36(1)：35－40.

[24] WANG T，DUONG T D，CHEN C C. Intention to disclose personal information via mobile applications：a privacy calculus perspective

[J]. International journal of information management, 2016, 36 (4):531－542.

[25] BANSAL G, ZAHEDI F M, GENFN D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online[J]. Decision support systems, 2010, 49 (2):138－150.

[26] 兰晓霞.移动社交网络信息披露意愿的实证研究——基于隐私计算与信任的视角[J].现代情报，2017，37(4):82－86.

[27] 李琪，王璐瑶，乔志林.隐私计算与社会资本对移动社交用户自我披露意愿的影响研究——基于微信与微博的比较分析[J]. 2018，37(5):169－175.

[28] GEFEN D. It is not enough to be responsive: the role of cooperative intentions in MRPⅡ adoption[J]. Database for advances in information systems, 2000, 31 (2): 65－79.

[29] MOOAMAN C, ZALTMAN G, DESHPANDE R. Relationships between providers and users of marketing research: the dynamics of trust within and between organizations[J]. Journal of marketing research. 1992, 29(3): 314－328.

[30] JARVENPAA S L, TRACTINSKY N. Consumer trust in an internet store: a cross-cultural validation [J]. Journal of computer-mediated communication, 1999, 5(2):1－33.

[31] RIFON N J, LAROSE R, CHOI S M. Your privacy is sealed: effects of web privacy seals on trust and personal disclosures[J]. Journal of consumer affairs, 2006, 39(2):339－362.

[32] HOFFMAN D L, NOVAK T P, PERALTA M. Building consumer trust online[J]. Communications of the ACM, 1999, 42(4):80－85.

[33] 张玥，孙霄凌，陆佳莹，等.基于隐私计算理论的移动社交用户信息披露意愿实证研究——以微信为例[J].图书与情报，2018 (3):90－97.

[34] 朱侯，王可，严芷君，等.基于隐私计算理论的SNS用户隐私悖论现象研究[J].情报杂志，2017，36(2): 134－139，121.

[35] YANG K. Consumer technology traits in determining mobile shopping adoption: an application of the extended theory of planned behavior[J]. Journal of retailing & consumer services, 2012, 19 (5): 484－491.

[36] 张晓娟，李贞贞.信息隐私关注、信任与智能手机用户的个人信息安全行为意向[J].现代情报，2018，38(3):45－50.

[37] CAVUSOGLU H, PHAN T Q, CAVUSOGLU H, et al. Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook[J]. Information systems research, 2016, 27 (4):848－879.

[38] 张会平，杨京典，汤志伟.社交媒体用户信息隐私关注的形成机制研究[J].情报理论与实践，2017，40 (6):40－43.

[39] LIU Z, WANG X. How to regulate individuals' privacy boundaries on social network sites: a cross-cultural comparison[J]. Information & management, 2018, 55(8):1005－1023.

[40] 李凯，黄敬尧，王晓文.LBS用户信息公开意愿影响因素分析——基于交换理论的实证研究[J].情报学报，2016，35(1): 84－97.

[41] XU H, DINEV T, SMITH H J, et al. Examining the formation of individual's information privacy concerns: toward an integrative view [C]//Proceedings of the 29th International Conference on Information Systems. Paris: AIS Electronic Library, 2008:14－17.

[42] FOGEL J, NEHMAD E. Internet social network communities: risk taking, trust, and privacy concerns [J]. Computers in human behavior, 2009, 25(1):153－160.

[43] KRASNOVA H, SPIEKERMANN S, KOROLEVA K, et al. Online social networks :why we disclose[J]. Journal of information technology, 2010, 25(2):109－125.

[44] PAVLOU P A, CHELLAPPA R K. The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions[D]. Los Angeles: Marshall School of Business, USC, 2001.

[45] KEHR F. Feeling and thinking: on the role of intuitive processes in shaping decisions about privacy[D]. St. Gallen: University of St. Gallen, 2015.

[46] SCHIERZ P G, SCHIKLE O, WIRTZ B W. Understanding consumer acceptance of mobile payment services: an empirical analysis [J]. Electronic commerce research and applications, 2010, 9 (3): 209－216.

[47] 199IT中文互联网数据咨询中心.2017年中国移动社交用户洞察报告[EB/OL].[2018－11－01]. http://www.199it.com/archives/609904.html.

作者贡献说明：

郭海玲：提出选题，确定研究思路，撰写论文，修改论文并定稿；

马红雨：论文撰写，文献查阅、数据收集及分析；

许泽辉：数据收集及分析。

Construction and Demonstration of the Influence Model of Social Media Users' Information Disclosure Intention: A Case Study of WeChat Users

Guo Hailing Ma Hongyu Xu Zehui

School of Management, Hebei University, Baoding 071002

Abstract: [**Purpose/significance**] Information privacy leakage incidents of social media occur frequently, which aggravates users' concerns about information privacy. Whether users are willing to disclose personal information to the

platform in the process of using social media has become the key to promote the healthy development of social media platforms. [**Method/process**] Based on privacy calculus theory and communication privacy management theory as the framework, combining privacy concerns, the paper constructed a model of the influence of users' willingness to disclose information on social media. Taking WeChat platform as the research object, the paper collected sample data by questionnaire survey, and used Smart PLS software to verify the rationality of the model. [**Result/conclusion**] The paper find that perceived benefits, trust and perceived information control all positively affect the information disclosure intention, while privacy concerns negatively affect the information disclosure intention. Trust has a negative impact on perceived risk. Perceived information control has a negative impact on privacy concern, and disposition to value privacy positively influences privacy concern and perceived risk.

Keywords: social media　privacy calculus　communication privacy management　information privacy　disclosure intention